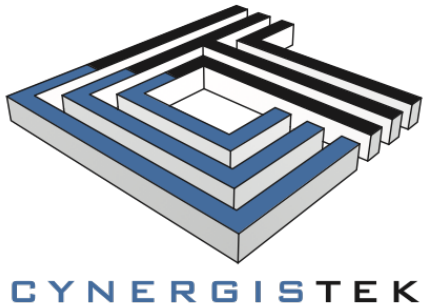
Managing Risk Related to Information Security in Healthcare



Presented By:

Mac McMillan | CEO, CynergisTek, Inc.

CUSTOMER RATED KLAS REVIEWED

CynergisTek was recognized in the 2016 KLAS Security Advisory Services report for having the highest overall client satisfaction, performance and impact on security preparedness in healthcare.

BEST IN KLAS SOFTWARE & SERVICES 2017

CynergisTek won the 2017 Best in KLAS Award for Cyber Security Advisory Services

CUSTOMER RATED KLAS REVIEWED

CynergisTek was recognized in the 2018 KLAS Cybersecurity Services Report as the company having the greatest breadth of security services and received high praise for their healthcare knowledge and executive involvement.

Today's Presenter

- CEO & President, CynergisTek, Inc.
- Recognized as leading expert in healthcare cybersecurity & compliance
- Former Chair, HIMSS P&S Committee & Policy Task Force
- Board Member CHIME/AEHIS
- Member multiple Advisory Boards
- Director of Security, for two DoD Agencies
- Excellence in Government Fellow
- HIMSS Fellow
- U.S. Marine Intelligence Officer, Retired

Mac McMillan
CEO - CynergisTek, Inc.
mac.mcmillan@cynergistek.com
512.402.8555

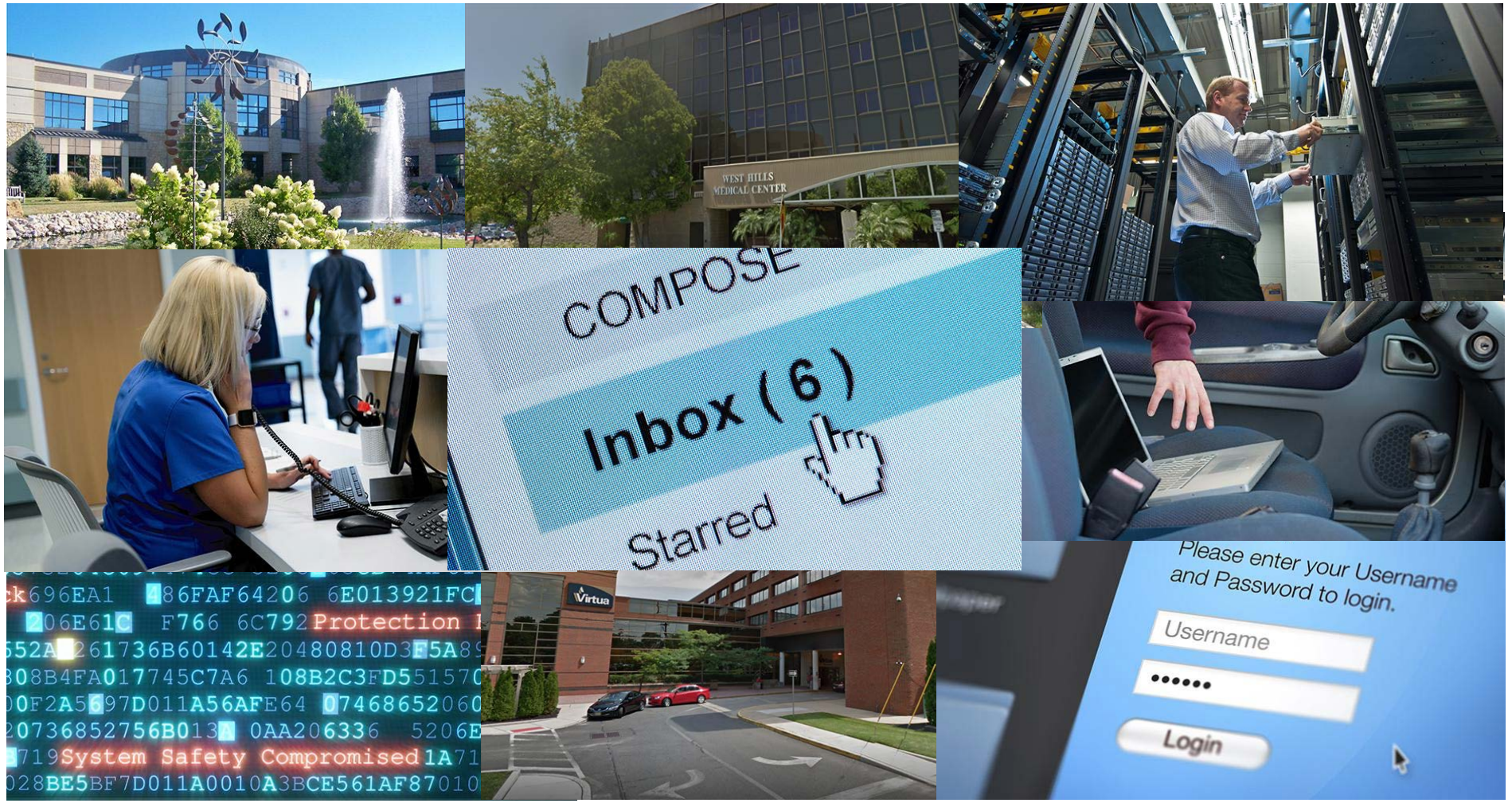
Why Cybercriminals Like Healthcare

Valuable Information

Lack of investment & Training

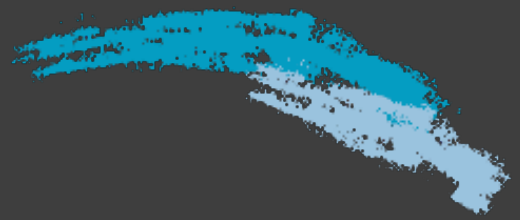
Highly Connected Systems

The New Reality of Healthcare



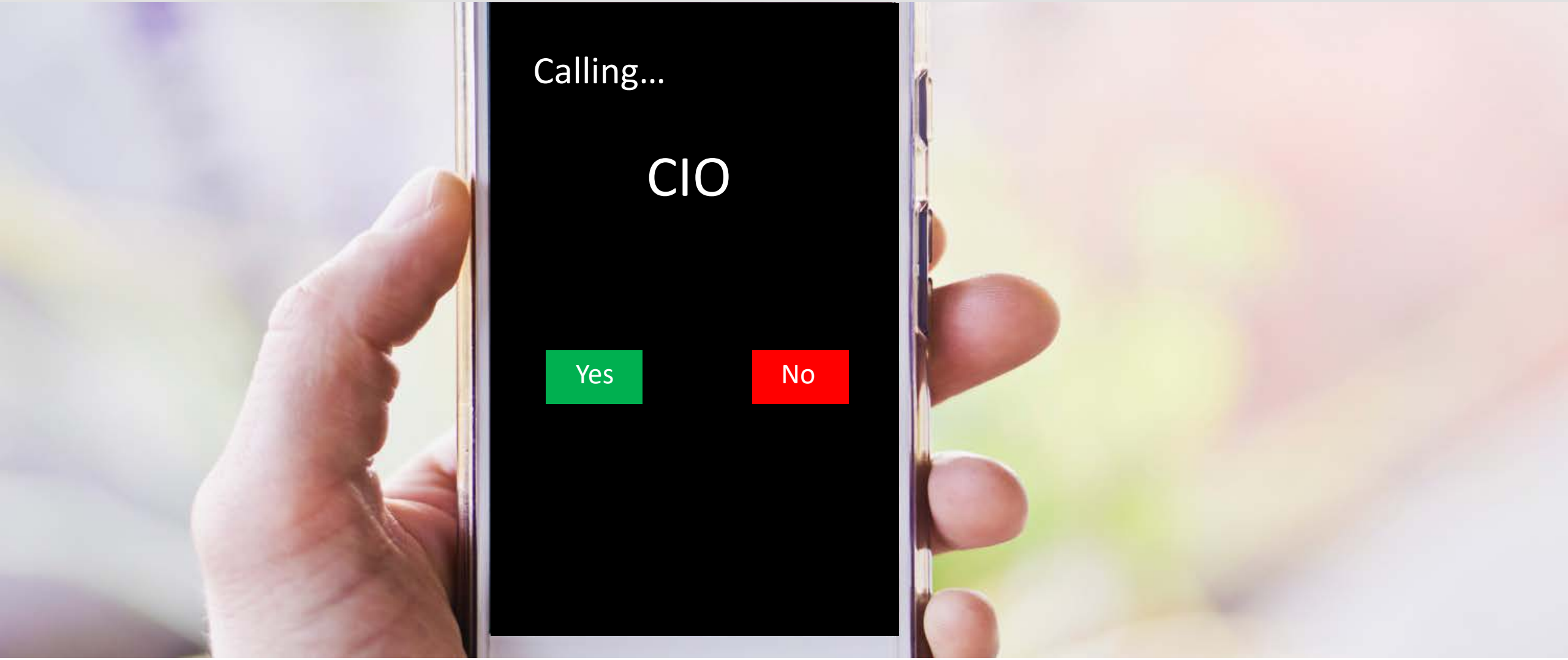
- Ransomware
- Phishing
- Hacked Workstation
- FTP Server Misconfigured
- Website Breach
- Database Misconfigured
- Email Breach
- Malware attack
- Stolen Laptop

Imagine….



Your CEO Getting Ready For An Evening Out

An After Hours Call… Never Good News



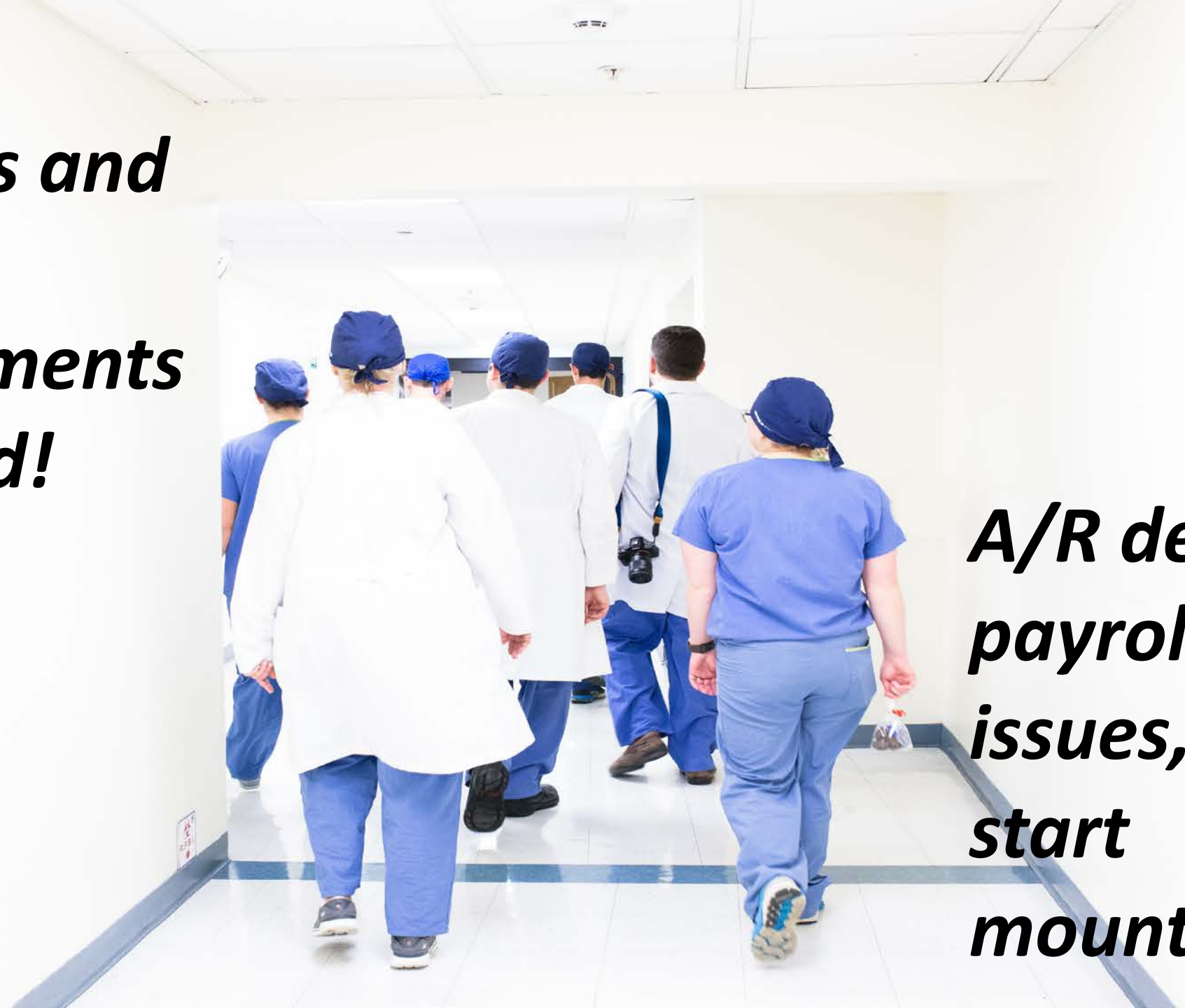
How Bad Could It Be…

Pretty Bad…


Your personal files are encrypted by CTB-Locker.
Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.
You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.
Press 'View' to view the list of files that have been encrypted.
Press 'Next' for the next page.
WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
View
95:59:29
Next >>

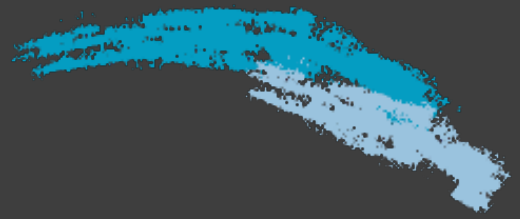

POL

Elective surgeries and general appointments cancelled!



A/R delays, payroll issues, costs start mounting!

The Impact



Impact on Operations

- Two full weeks of downtime – enterprise-wide
- Opened Incident Command Center – 24/7
- Paper processing for nearly everything
- Younger staff were often clueless – “Thank God for older nurses!”
- Needed many “runners” to go everywhere (pick up lab orders, etc.)
- Confusion and inconsistency re: backloading of data/charges
- “Downtime Boxes” were designed for 2-3 days
  - Ran out of forms and prescription pads
  - Used print shop for what they could
  - Old versions of paper order sets

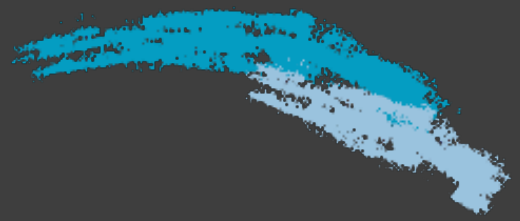
Impact on Operations

- Phones initially impacted (on the same network)
  - Lost ACD/Menu functionality for several days
- OR Schedule reviewed for “elective” or “postpone-able” procedures
  - No PACS availability – Access to images a challenge
- BCA Devices – lost nearly all value after a couple of days
- IT directed to focus on Payroll and Materials Mgmt.
  - You have to pay your staff and order your supplies
- EMR was never actually infected – but limited workstation access made it virtually unusable/inaccessible
  - Focused on a few workstations in order to maintain up to date census

Impact on People

- Staff burn-out, mistakes, stress, irritability
- Forced a few “stay home” days for some staff
- Stress/Worry that any negative patient outcome would be “our” fault
- Stress/Worry about missing something critical increases
  - Access to servers/databases with critical cancer regimen data
  - Access to old clinical data/images
  - Access to allergy data, etc.
- “Remediation Services” not what was expected
  - Required obtaining extra staff from peer organizations and temp agencies

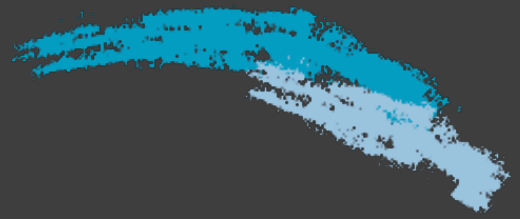
The Recovery



The Recovery

- 14 *days* of paper orders, charges, results, etc.
- 4+ *months* of matching patients with orders, charges, and results in the system
- Additional expense of $250K - $500K (overtime, special services, remediation assistance) not counting new security hardware or software
- No claims processing for 60+ days – No incoming cash flow
- Revenue reduction (lost revenue) of $2 million
- No progress on IT projects for several months

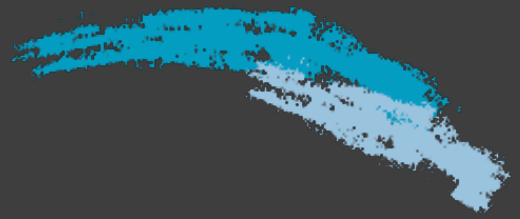
The Cleanup



The Cleanup

- Took a solid four months of enterprise-wide effort, but…
- It is *still* happening six months post event
- Confusion and inconsistency of cleanup process
  - Some departments and clinics entered their own backload of data
  - Others had ancillary departments enter their orders/charges
  - Still a few others did nothing, causing frustration and delays
    - *"Lab gets the revenue, they should do the work"*
    - *"Who has the paperwork now?"*
    - *"Our staff doesn't want the extra overtime or weekend work"*
    - *"We didn't cause this, why should we have to fix it?"*
- We still occasionally find a missing charge, order, or result

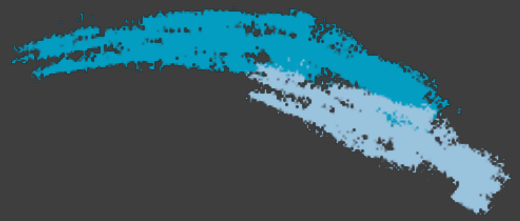
The Post Mortem



The Post Mortem

- Need to reconsider “downtime” box contents, plan for longer outage
- Need to test all BCA devices and off-line printing capabilities
- Need to add more BCA devices, and downtime computer workstations
- Leadership, Department, and Physician contact lists were a) out of date, and b) hard to find (when network is down)
- Need to quickly establish mini-registration/census location(s) and distribute information often
- Need better access to standardized forms
- Need better access to paper-based order sets
- Need a formal plan for who will do what (backloading of orders, charges, results) and other scanning

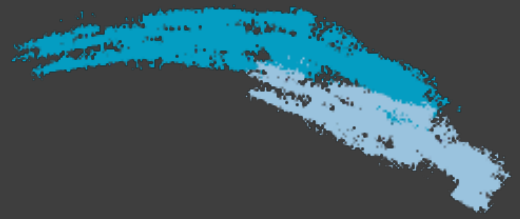
Lessons Learned



Lessons Learned

- The financial recovery following a ransomware event takes a minimum of six months, and even then, the unrecoverable costs are often measurable in the millions. *A Ransomware Post Mortem*, Clyde Hewitt, Health Management Technology, March-April 2018
- 25% of patients have changed their provider following a major data breach Accenture, 2017 Consumer Survey on Cybersecurity and Digital Trust.
- U.S. organizations that paid the ransoms were targeted and attacked again with ransomware 73 percent of the time. Business Wire March 27, 2018
- Forty five percent of U.S. companies hit with a ransomware attack last year paid at least one ransom; but only 26 percent of these companies had their files unlocked. Business Wire March 27, 2018

Todays' Threats



The Cyber Landscape Has Changed

- In 2017, less than 1 in 10 providers had not adopted an EHR system, compared to the inverse in 2003
- Hacking has increased several hundred percent since 2015
- Ransomware attacks soared to 80,000 an hour in 2017, falling off in 2018 only to be replaced by cryptomining, phishing and more advanced malware attacks
- Breaches today are more about disruption and destruction of data rather than simple theft of data or extortion
- And the new concern is data corruption, the silent attacker

Top Security Risks in Healthcare

Theft & Loss

Nearly half of all breaches involve some form of theft or loss of a device not properly protected or paper.

Insider Abuse

Breaches in healthcare continue to be carried out by knowledgeable insiders for identity theft, tax fraud, and financial fraud.

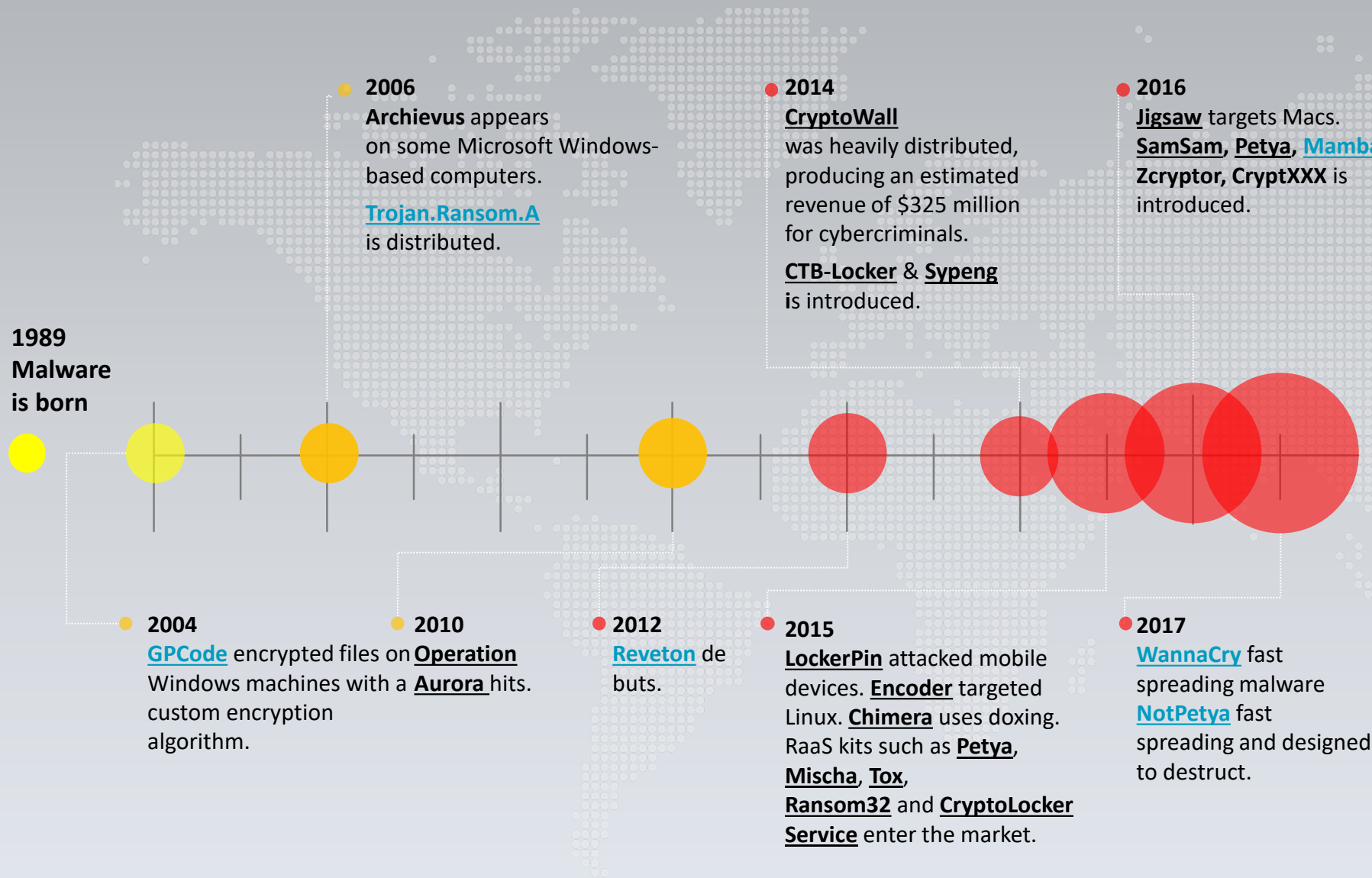
Unintentional Action

Breaches caused by mistakes or unintentional actions such as improper mailings, errant emails, or facsimiles are still prevalent.

Cyber Attacks

Majority of large breaches reported in 2017 involved some form of hacking and represented nearly 99% of the records compromised.

Attacks are growing in frequency



- Every time a new smartphone is turned on, the digital attack surface grows. Every time a new device is connected to the Internet of Things (IoT), the cyber landscape becomes less secure.

  – McKinsey & Company

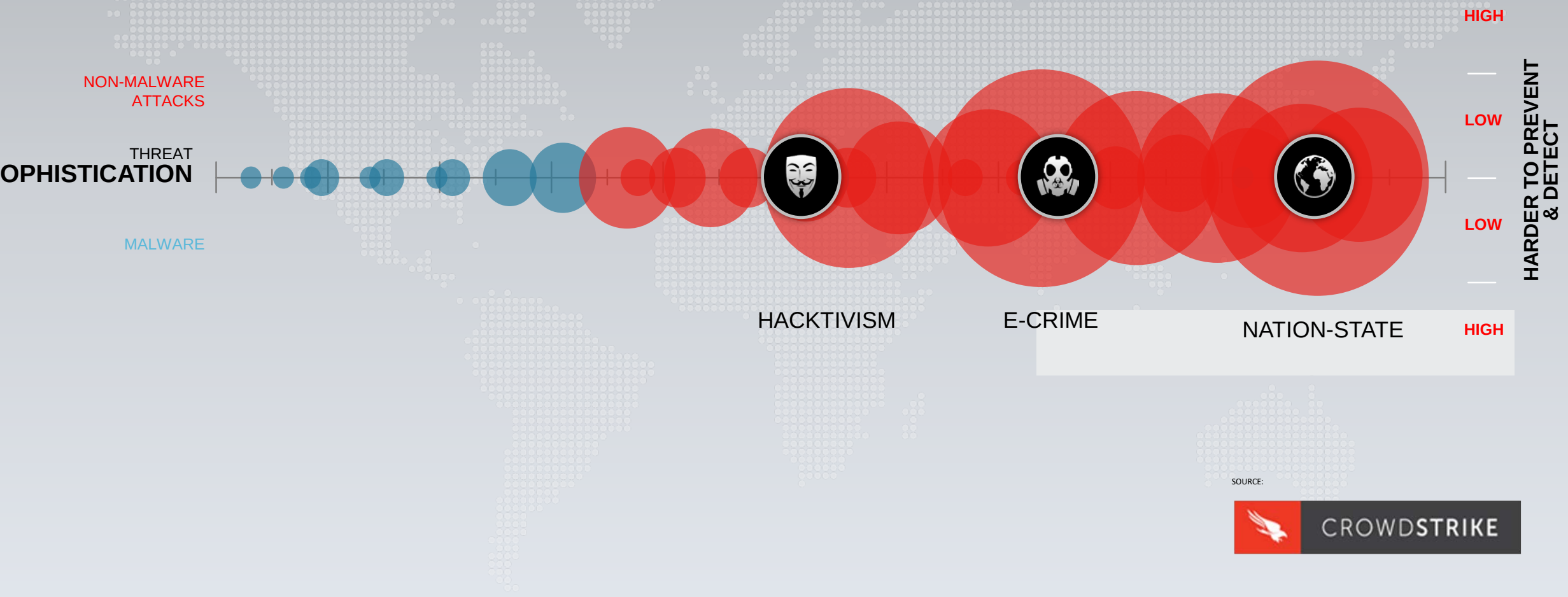
- Industry experts estimates healthcare cyberattacks rose 320% between 2015 and 2016.
- Healthcare has emerged as the most frequently targeted industry, with 164 threats detected per 1,000 host devices.

  – Vectra Networks Industry Report 2017

- Accordingly, health care cybersecurity spending is expected to reach nearly $65 billion by 2021.

  – Cybersecurity Ventures 2017

Attacks are growing in sophistication



SOURCE:

CROWDSTRIKE

Changing Risk Priorities

From "Business Critical" to "Mission Critical" to "Life Critical"

Confidentiality

- PHI (HIPAA)
- But also PII & PCI
- Account Information
- Billing & Payment Data
- Intellectual Property
  - Clinical Trials
  - Research
  - Design & Formularies
- Legal & HR Documents
- Identities & Credentials

Availability

- Clinical Systems
  - EHR & Specialty
  - Ancillary (PACS, Lab, Pharma)
  - ePrescription / EPCS
- Medical Devices
  - Availability of clinical services and results
- Business Systems
  - Email
  - Billing, Scheduling

Integrity

- Critical Patient Data
  - Prescriptions, Medications
  - Dosages
  - Allergies
  - History
  - Diagnosis
  - Alarms
- Critical Technical Data
  - Calibration
  - Safety Limits

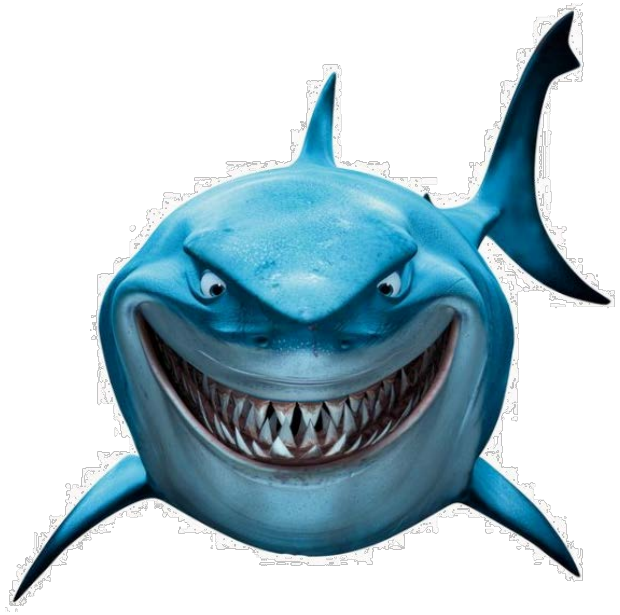
Patient Experience: "Patient Trust Zone"

Patient Harm: "Patient Safety Zone"

Managing Cybersecurity is Challenging

- "More people are killed every year by pigs than by sharks, which shows you how good we are at evaluating risk."

  Schneier, Bruce. Interview with Doug Kaye. IT Conversations: Bruce Scheier. 2004-04-16.

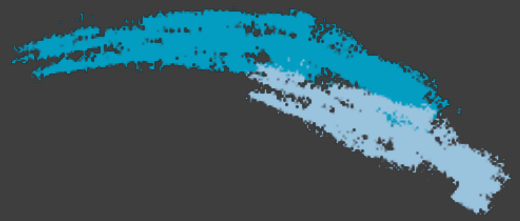


Are We Ready?

60% of IT security experts who responded to the Black Hat Attendee Survey believe that a successful attack on U.S. critical infrastructure will happen within two years. Also, only 26% of respondents believe that the country is prepared to handle such an attack.

Dark Reading, July 10, 2017

A Parting Thought



I See You…

SHODAN

Shodan = Google for Hackers

Thank You!

Mac McMillan, FHIMSS, CISM
President & CEO
mac.mcmillan@cynergistek.com
512.402.8555